IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.	: 10/786,224	Confirmation No.	: 2832
First Named Inventor	: Burkhard KUHLS		
Filed	: February 26, 2004		
TC/A.U.	: 2136		
Examiner	: JOHNSON, CARLTON		
Docket No.	: 080437.53236US		
Customer No.	: 23911		
Title	: Method for Providing Software to Be Used by a Control Unit of a Vehicle		

REPLY AFTER FINAL

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the final Office Action dated November 28, 2007, reconsideration and allowance of the above-identified application are respectfully requested. Claims 1-20 remain pending.

Claims 1-20 are rejected under 35 U.S.C. § 103(a) as being obvious in view of the combination of U.S. Patent No. 5,957,985 to Wong et al. ("Wong") and U.S. Patent No. 6,463,535 to Drews ("Drews"). This ground of rejection is respectfully traversed.

Applicant's claim 1 recites a method that involves *signing software* against falsification using a secret key according to a public-key method and checking the *signed software* for integrity using a public key complementary to the secret key. The combination of Wong and Drews does not disclose or suggest this claimed method.

The Office Action recognizes that Wong does not even mention signing software or checking the integrity of signed software, and instead relies upon Drews for such a disclosure. For the reasons set forth below, it is respectfully submitted that Drews does not remedy the deficiencies of Wong with respect to Applicant's claim 1.

THE DISCLOSURE OF DREWS

Drews discloses a method of verifying the integrity of a boot image, and whether the boot image is authorized to be executed by a local platform[1]. A boot image 140 and signed manifest 150 are downloaded from a central platform 110 to the local platform 120[2]. Integrity of the boot image is verified by calculating a hash value of the downloaded boot image and comparing this calculated hash value with a secure hash value contained in the signed manifest[3].

The secure hash value contained *in the signed manifest* is generated by loading portions of the boot image into a one-way hash function that produces the hash value[4]. A number of hash values of *the signed manifest* are appended end-to-end to produce a hash set, and this hash set is digitally signed[5].

---

[1] Abstract and column 4, lines 4-12.
[2] Column 3, lines 18-24.
[3] Column 5, lines 55-58.
[4] Column 4, lines 38-42.
[5] Column 4, lines 45-50.

Calculation of the hash value of the download boot image is accomplished by applying the hash function used to produce the secure hash value to the boot image[6]. Drews does not, however, disclose or suggest that the downloaded boot image is:

- signed against falsification;
- signed using a secret key; or
- checked for integrity using a public key complimentary to the secret key.

THE OFFICE ACTION'S CITATIONS TO DREWS

The final Office Action includes a number of citations to Drews for the disclosure of the aforementioned elements of Applicant's claim 1. As will be described below in detail, however, there is nothing in these sections disclosing the aforementioned claim elements.

Column 4, lines 31-38 and 48-54

The Office Action cites these portions of Drews as disclosing "sign software; utilizing private key, PKI technique."[7] Column 4, lines 31-38 is reproduced below[8]:

---

[6] Claim 5.
[7] Page 2, paragraph 3.1 and page 6.
[8] *Emphasis added.*

> Referring to FIG. 3, an illustrative block diagram *of signed manifest 150* corresponding to boot image 140 is shown. *Signed manifest 150 includes* (i) a secure hash value 300 for each sub-image of the boot image, (ii) a manifest digital signature 310, and (iii) a certificate chain 320 providing the identify of the signatory of signed manifest 150 and those entities which have bestowed signing authority to the signatory. In this particular, embodiment, each secure

As can be clearly seen by reviewing the cited portion of Drews reproduced above, this portion discusses *signed manifest 150* and *not the boot image.* Accordingly, there is nothing in this section disclosing or suggesting signing the boot image.

Column 4, lines 48-54 is reproduced below[9]:

> number, M≥1) to provide a hash set 330. Thereafter, *hash set 330 is digitally signed* with a private key (PRKS) of the source authorized to provide the boot image. Herein, the functions used for digitally signing information include Rivest Shamir Adleman (RSA) by RSA Data Security, Inc. of Redwood City, Calif. and the Digital Signature Algorithm (DSA) proposed by the National Institute of Standards. Both

This section of Drews describes digitally *signing hash set 330*, which is part of the *signed manifest*, and not part of the boot image. Accordingly, there is nothing in this section of Drews disclosing or suggesting *digitally signing the boot image.*

[9] *Emphasis added.*

Column 4, lines 1-6, lines 9-14 and Column 4, lines 23-26

The Office Action cites these portions of Drews as disclosing "verify (check) signature with public key (complimentary to private (secret) key), validity check."[10]

Column 4, lines 1-6 is reproduced below:

> In this embodiment, as further shown in detail in FIG. 5A and 5B, verification function 270 includes software, executed by the local platform during pre-boot, in order to perform an integrity check procedure. The integrity check procedure verifies that a boot image has not been modified since the signed manifest was created. Thus, modifications

This section of Drews describes that an integrity check is performed to verify that the boot image has not been modified. There is nothing, however, in this section disclosing or suggesting that the boot image *is signed.*

Column 4, lines 9-14 is reproduced below[11]:

> the local platform. As an optional feature, the verification function 270 further performs an *authorization check procedure* to determine whether the boot image has been provided by an acceptable source. The *authorization check procedure* is performed when authorization check enable flag 290 is enabled.

This section of Drews describes an authorization procedure to check that the boot image is provided by an acceptable source, a completely different

[10] Page 2, paragraph 3.1.

procedure from the verification of integrity procedure described above. Nevertheless, there is nothing in this section disclosing or suggesting that the authorization procedure *involves a signed boot image.*

Column 4, lines 23-26 is reproduced below[12]:

> the boot image. Confirmation on whether or not the source is authorized to provide the image is determined through analysis of the *signed manifest* using the public key provided by authorization certificate 280. It is contemplated that

This section of Drews describes the authorization procedure, and not the verification of integrity procedure. Furthermore, this section only describes that the *manifest is signed*, but does not disclose or suggest that the *boot image is signed.*

Having shown that each portion of Drews cited by the Office Action does not support the position that Drews discloses or suggests the use of signed software, it is respectfully submitted that Applicant has established that Drews does not disclose or suggest the use of signed software. Because the rejection of Applicant's claim 1 relies upon Drews for the disclosure of signed software, it is respectfully submitted that the combination of Wong and Drews does not render Applicant's claim 1 obvious.

---

[11] *Emphasis added.*
[12] *Emphasis added.*

Dependent claims 2-6 and 8-18 are patentably distinguishable over the combination of Wong and Drews at least by virtue of their dependency from claim 1.

Independent claims 7 and 19 recite methods involving signed software, and are patentably distinguishable over the combination of Wong and Drews for similar reasons to those discussed above with regard to claim 1. Claim 20 is patentably distinguishable over the combination of Wong and Drews at least by virtue of its dependency from claim 19.

Moreover, as discussed in Applicant's previous Reply, the combination of Wong and Drews does not disclose or suggest the specific certificates recited in claim 7. The final Office Action provides a definition of a certificate and appears to rely upon the certificate chain 320 of the signed manifest 150 as disclosing these specific certificates[13].

Drews does not, however, disclose or suggest that the certificates in the certificate chain 320 include the claimed clearing code site signature certificate and a software signature certificate. A generic disclosure of certificates does not satisfy the evidentiary burden necessary to establish obviousness of the specific certificates recited in Applicant's claims. Accordingly, the combination of Wong and Drews does not render claim 7 obvious for this additional reason.

[13] It is noted that the definition of a certificate provided in the Office Action does not appear to be consistent with the definition provided in column 2, lines 59-66 of Drews.

For at least those reasons stated above, it is respectfully requested that the rejection of claims 1-20 as being obvious in view of the combination of Wong and Drews be withdrawn.

If there are any questions regarding this response or the application in general, a telephone call to the undersigned would be appreciated since this should expedite the prosecution of the application for all concerned.

If necessary to effect a timely response, this paper should be considered as a petition for an Extension of Time sufficient to effect a timely response, and please charge any deficiency in fees or credit any overpayments to Deposit Account No. 05-1323 (Docket # 080437.53236US).

Respectfully submitted,

January 14, 2008

Stephen W. Palan
Registration No. 43,420

CROWELL & MORING, LLP
Intellectual Property Group
P.O. Box 14300
Washington, DC 20044-4300
Telephone No.: (202) 624-2500
Facsimile No.: (202) 628-8844
SWP:crr
4807115